

HISPOL 003.0

The United States House of Representatives Information Security Policy for Connecting to the House Local Area Network

Version:	3.0
Approved:	January 2010
Approval Authority:	The United States House of Representatives Committee on House Administration

Table of Contents

1	Introduction.....	3
	1.1 SCOPE	3
2	Policy Guidelines	3

1 Introduction

The goal of this policy is to minimize internal and external security threats to House information systems while allowing House Offices to use the campus Intranet, Internet, and other external networks to the maximum extent feasible.

1.1 Scope

This document provides all users of House information systems with guidance governing permanent connections to the House network. All House Offices, employees, and contractors that connect to the House network and utilize House information systems must follow this guidance since improper use of information systems may put the entire House network at risk.

2 Policy Guidelines

All House Offices must notify the Information Systems Security Office (INFOSEC) when connecting systems to the House network. Systems will be reviewed to determine compliance with security policy and technical controls as described in House Information Security Policies (HISPOLs) and Publications (HISPUBs). . If significant vulnerabilities are identified, corrective action must be taken within the time period specified by INFOSEC.

The following guidelines apply:

- 1) Any device or component with a permanent connection to the House network shall be used for authorized purposes, only, and may not be used for campaign, political, or commercial activities. Use of such devices and components must comply with House Rules and the guidance of the Committee on Standards of Official Conduct.
- 2) Any device or component with a permanent connection to the House network, or to the overall House infrastructure must be reviewed and approved to minimize the potential for security risks and violations.
- 3) Permanent connections to the Internet outside of the House infrastructure must be reviewed and approved by INFOSEC. All Internet access and servers attached to the House network must comply with House policies, procedures, technical specifications, and guidelines and must pass through the House maintained security infrastructure.
- 4) All wireless connections must follow the technical and procedural guidelines contained in HISPUB 6.1.
- 5) Only Members, Officers, and employees are authorized to connect to the House network using a permanent connection, as defined in this policy.

- 6) Modems are not permitted for use at the House, except when connected to a fax machine, unless authorized by INFOSEC, . The devices may be used to bypass security features such as firewalls designed to keep unauthorized users from accessing the network.
- 7) All House Office information systems connecting to the House network infrastructure must be physically and logically isolated from vendors external to the House and all other non-House networks, unless explicitly validated by INFOSEC.
- 8) All House offices must ensure that servers are located within areas of minimal public and visitor traffic.
- 9) All House Offices authorized with a permanent connection to the network and access to the Internet must designate a central point of contact (POC) for all matters pertaining to their connection. In most cases, the system administrator is the designated POC.
- 10) All new public web sites for Members or Committees must be hosted on a server managed by HIR, or by an authorized vendor if the server is located on the House Campus.
- 11) A mail server may only use approved House mail relay servers if the message originates from a computer physically connected to the House network. No mail server shall be allowed to utilize third party mail systems for any Simple Mail Transfer Protocol (SMTP) traffic outside of the House domain. This policy is enforced at the House firewalls.
- 12) All programs used on the system must be checked prior to installation for viruses or other malicious forms of code. This is especially important for programs received from outside sources, including the Internet. Each House Office must have the House-provided or an equivalent current anti-virus program installed on their systems.
- 13) It is the responsibility of each House Office to contact INFOSEC and report security incidents such as unauthorized access or unusual system activities to the House Computer Incident Response Team (House CIRT). The House CIRT will conduct an investigation, provide recommendations to resolve the incident, and follow up with the designated POC to ensure corrective actions are completed.